IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A system for automatically protecting private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium;

a decryption module retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption;

a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium;

a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash;

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

2. (Cancelled)

3. (Previously Presented) A system according to Claim 1, further comprising:

an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

4. (Cancelled)

5. (Original) A system according to Claim 1, further comprising:

an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

6. (Original) A system according to Claim 5, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

7. (Original) A system according to Claim 1, further comprising:

a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

8. (Cancelled)

9. (Cancelled)

10. (Currently Amended) A method for automatically protecting private video content using embedded cryptographic security, comprising:

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium;

retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption;

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key;

generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame and comparing the verification cryptographic hash and the original cryptographic hash;

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

11. (Cancelled)

12. (Previously Presented) A method according to Claim 10, further comprising:

providing an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

13. (Cancelled)

14. (Original) A method according to Claim 10, further comprising:

providing an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

15. (Original) A method according to Claim 14, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

16. (Original) A method according to Claim 10, further comprising:

providing a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

17. (Cancelled)

18. (Cancelled)

19. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 10, 12, 13, 14, 15 or 16.

20. (Currently Amended) A system for encrypting private video content using embedded cryptographic security, comprising:

a frame buffer receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

a processor encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair; and

a recorder storing the encrypted frames on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair,

wherein the processor generates a fixed-length original cryptographic hash from at least one such individual frame and encrypts the original cryptographic hash using an encryption cryptographic key selected from the cryptographic key pair and the recorder stores the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair,

wherein at least one of the encryption cryptographic key and the decryption cryptographic key is stored on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

wherein the decryption key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions is stored on the removable storage medium and employs at least one of the encryption key and the decryption key;

wherein only encrypted video content passes a first physical boundary separating the recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

21. (Cancelled)

22. (Previously Presented) A system according to Claim 20, further comprising:

a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

23. (Original) A system according to Claim 20, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

24. (Original) A system according to Claim 20, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

25. (Cancelled)

26. (Currently Amended) A method for encrypting private video content using embedded cryptographic security, comprising:

receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair;

storing the encrypted frames on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key selected from the cryptographic key pair;

storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair;

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

validating the decryption key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption key and the decryption key on the removable storage medium;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

27. (Cancelled)

28. (Previously Presented) A method according to Claim 26, further comprising:

employing a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

29. (Original) A method according to Claim 26, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

30. (Original) A method according to Claim 26, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

31. (Cancelled)

32. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 26, 28, 29, or 30.

33. (Currently Amended) A system for decrypting private video content using embedded cryptographic security, comprising:

a player retrieving encrypted frames from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair;

a frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form,

wherein the player retrieves a digital signature from the transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from the cryptographic key pair, and the processor decrypts the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair, generates a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium, and compares the verification cryptographic hash and the original cryptographic hash; and

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions is stored on the removable storage medium and employs at least one of the encryption cryptographic key and the decryption cryptographic key;

<u>wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;</u>

<u>wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from the player;</u>

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

34. (Cancelled)

35. (Previously Presented) A system according to Claim 33, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

36. (Original) A system according to Claim 33, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

37. (Original) A system according to Claim 33, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

38. (Cancelled)

39. (Currently Amended) A method for decrypting private video content using embedded cryptographic security, comprising:

retrieving encrypted frames from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair;

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

retrieving a digital signature from the transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from the cryptographic key pair;

decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium and comparing the verification cryptographic hash and the original cryptographic hash;

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

40. (Cancelled)

41. (Cancelled)

42. (Original) A method according to Claim 39, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

43. (Original) A method according to Claim 39, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

44. (Cancelled)

45. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 39 or 42.

46. (Currently Amended) A system for automatically authenticating private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key comprising a private key of an asymmetric cryptographic pair, and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

a verification module retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key comprising a public key of an asymmetric cryptographic pair;

a player frame buffer generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption

cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

47. (Cancelled)

48. (Previously Presented) A system according to Claim 46, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

49. (Cancelled)

50. (Cancelled)

51. (Currently Amended) A method for automatically authenticating private video content using embedded cryptographic security, comprising:

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form and

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key comprising a private key of an asymmetric cryptographic pair and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key comprising a public key of an asymmetric cryptographic pair;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

52. (Cancelled)

53. (Previously Presented) A method according to Claim 51, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

54. (Cancelled)

55. (Cancelled)

56. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claim 51.

57. (Currently Amended) A system for digitally signing private video content using embedded cryptographic security, comprising:

a frame buffer receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

a processor generating a fixed-length original cryptographic hash from at least one such individual frame and encrypting the original cryptographic hash using an encryption cryptographic key selected from a cryptographic key pair;

a recorder storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair; and

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions is stored on the removable storage medium and employs at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein only encrypted video content passes a first physical boundary separating the recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

58. (Original) A system according to Claim 57, further comprising:

a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

59. (Cancelled)

60. (Currently Amended) A method for digitally signing private video content using embedded cryptographic security, comprising:

receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key selected from a cryptographic key pair;

storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair;

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the individual frames;

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

61. (Original) A method according to Claim 60, further comprising:

employing a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

62. (Cancelled)

63. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claims 60 or 61.

64. (Currently Amended) A system for verifying digitally signed private video content using embedded cryptographic security, comprising:

a player retrieving a digital signature from a transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair, generating a verification fixed-length cryptographic hash from at least one individual frame retrieved

from the transportable storage medium, and comparing the verification cryptographic hash and the original cryptographic hash;

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the at least one individual frame;

wherein the decryption cryptographic key is validated against user-provided credentials prior to decrypting the encrypted frames;

wherein a set of cryptographic instructions is stored on the removable storage medium and employs at least one of the encryption cryptographic key and the decryption cryptographic key;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from the player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

65. (Original) A system according to Claim 64, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

66. (Cancelled)

67. (Currently Amended) A method for verifying digitally signed private video content using embedded cryptographic security, comprising:

retrieving a digital signature from a transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium and comparing the verification cryptographic hash and the original cryptographic hash;

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium such that a plurality of encryption cryptographic keys, each associated with a different removable storage medium, are capable of being utilized for encrypting the at least one individual frame;

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames; and

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium;

wherein only encrypted video content passes a first physical boundary separating a recorder from the transportable storage medium;

wherein only the encrypted video content passes a second physical boundary separating the transportable storage medium from a player;

wherein only signed video content passes the first physical boundary separating the recorder from the transportable storage medium;

wherein only the signed video content passes the second physical boundary separating the transportable storage medium from the player.

68. (Cancelled)

69. (Cancelled)

70. (Previously Presented) A computer-readable storage medium holding code for performing the method according to Claim 67.